Motion Imagery Standards Board **Recommended Practice:** **Security Metadata Universal Set for Digital Motion Imagery**	**MISB RP 0102.2** 25 November 2003

1. Scope

This Recommended Practice (RP) describes the use of security metadata in MPEG-2 digital motion imagery applications. For applications involving national security it is mandatory that each part of a motion imagery file be marked correctly and consistently with security classification and other security administration information. The approved practices in this RP shall be applied to all MPEG-2 motion imagery implementations and shall be used to link security metadata to essence (video, audio, or data) and/or other metadata.

This RP defines only the format of embedding security metadata in MPEG-2 files. The methods used to gather security information, create files and insert security-metadata into files are the responsibility of application system developers. Similarly, the proper display of security information on screens, computer displays, printed output, etc. is the responsibility of system application developers. Originators and application users are responsible for the proper handling and ultimately for the use and disposition of classified information.

2. References

2.1. Normative References

Director of Central Intelligence, Community Management Staff, Controlled Access Program Coordination Office (CAPCO), *Intelligence Community Classification and Control Markings Implementation Manual*, 10 Sep 1999, amended 12 Oct 2000

Director of Central Intelligence Directive (DCID) 6/3, *Security Requirements For Interconnected Information Systems*, 4 Feb 2000

CAPCO Authorized Classification and Control Markings Register, 12 Oct 2000

SMPTE 335M-2001, *Data Encoding Protocol Using Key-Length-Value*

SMPTE 336M-2001, *Metadata Dictionary Structure*

SMPTE 330M, *Unique Material Identifier (UMID)*

SMPTE RP210-2001, *Metadata Dictionary*

ISO/IEC 13818-1:1996, *Information Technology – Generic coding of moving pictures and associated audio information: Systems* (commonly called MPEG-2 Systems)

MIL-STD-2500B, *National Imagery Transmission Format Version 2.1 for the National Imagery Transmission Format Standard*, 22 August 1997

ISO 3166-1, *Codes for the representation of names of countries and their subdivisions: Country Code*s, 1 October 1997 and updated by the ISO 3166 Management Authority (MA) at: http://www.din.de/gremien/nas/nabd/iso3166ma/codlstp1/index.html

Federal Information Processing Standards (FIPS) Publication 10-4, *Countries, Dependencies,*

Areas of Special Sovereignty, and Their Principal Administrative Divisions, National Institute of Standards and Technology, April 1995 (through Change Notice 6, 28 January 2001)

MISB Standard 0107, *Bit and Byte Order for Metadata in Motion Imagery Files and Streams*, 11 October, 2001

2.2. Informative References

MISB RP, *Use of MPEG-2 Systems Streams in Digital Motion Imagery Systems*

Director of Central Intelligence Directive 1/7, 30 Jun 1998

Executive Order 12958, Jun 1995

3. Introduction

This RP defines the contents and the application of a Security Metadata Set in digital motion imagery. The first section explains the individual elements in a Set that are normative in the Metadata Dictionary (SMPTE Standard 336M and SMPTE RP210). The construction of a Security Metadata Set from these elements follows SMPTE Standard 335M using the KLV metadata encoding protocol. Finally, this RP defines how the Security Metadata Set shall be used for tagging essence and other metadata sets in MPEG-2 Transport Streams (TS) and Program Streams (PS).

4. Security Metadata Set for Digital Motion Imagery

The sections of this RP are applicable only to MPEG-2 bitstreams. The practices shall be followed to ensure that all parts of an MPEG-2 TS or PS are tagged correctly with security information for use by applications. All metadata shall be represented using big-endian (most significant byte – MSB - first) encoding. Bytes shall be big-endian bit encoding (most significant bit – msb - first).

4.1. Security Metadata Elements

The following Security metadata elements comprise information needed to comply with CAPCO and other referenced security directives. These normative documents govern when certain fields are mandatory and when fields are optional. Table 1 is a summary of metadata elements within the Security Metadata Universal Set.

4.1.1. Security Classification

This metadata element contains a value representing the entire classification of the file. Possible values are: TOP SECRET, SECRET, CONFIDENTIAL, RESTRICTED, and UNCLASSIFIED (all caps).

This is the first section of the classification line. If the classification is US, then it is followed by a double forward slash "//". If the classifying country is Non-US the classification contains no slashes.

Example of US classification: **SECRET//**
Example of Non-US classification: **SECRET**

4.1.2. Non-US Classifying Country or Releasing Instructions Country Coding Method

This metadata element identifies the country coding method for the Non-US Classifying Country (Par. 4.1.3) and Releasing Instructions (Par. 4.1.5) metadata. The Country Coding Method shall use FIPS 10-4 two-letter or four-letter, alphabetic country code or ISO-3166 two-letter or three-letter codes. This metadata element is not needed if the default FIPS 10-4 two-letter code is used.

Example of Country Coding Method: **ISO-3166 Two Letter**

4.1.3. Non-US Classifying Country

This metadata element contains a value for the Non-US classifying country code preceded by a double slash "//." The default is the FIPS 10-4 two-letter code.

Example of Non-US classifying country: **//DEU** (Example of ISO-3166 code)
//UK (Example of default FIPS 10-4 code)

4.1.4. Caveats

This metadata element set contains a value representing all pertinent caveats/codewords from each category of he CAPCO register. These caveats form a field in the classification line marking. Entries in this field may be abbreviated or spelled out. This field shall be used to indicate FOR OFFICIAL USE ONLY or may be abbreviated as FOUO. It shall always be preceeded by the classification element containing the string UNCLASSIFIED// and shall not stand alone.

Examples of Caveats: **NOFORN**
REL TO
RELEASABLE TO
FOR OFFICIAL USE ONLY
FOUO

4.1.5. Releasing Instructions

This metadata element contains a valid list of country codes in accordance with ISO 3166 to be used to determine the countries to which a file or metadata is releasable. Country codes shall be separated by single blanks (spaces).

Example of Releasing Instructions: **USA DEU**
US UK

4.1.6. Declassification Date

Whether a date or a code indicating the category of exemption from declassification, this metadata element is always the last field in the classification marking string for classified information. The Declassification Date appears in two areas, the Classification Line, and in the lower right section of the first page of a file or document:

Examples of Declassification Date field: **20130801**
X1

4.1.7. Classified By

This metadata element identifies the name and type of authority used to classify the file. The metadata element is free text and can contain either the original classification authority name and

position or personal identifier, or the title of the document or security classification guide used to classify the material.

Example of Classified By field: **MGEN John Doe, Dir XLM**

4.1.8. Classification Reason

This metadata element contains the free text reason for classification or a citation from a document (see below).

Example of Classification Reason: **Par 1.5(a)**

4.1.9. Derived From

This metadata element contains that derivative information relating to a file or document and is free text. The metadata element is not needed if the "Classified by" authority has Original Classification Authority.

Example of Derived From: **Program XYZ Security and Classification Guide**

4.1.10. Classification or Marking System

This metadata element identifies the classification or marking system used in this Security Metadata Set. The entry shall be a free text field. This metadata element is not needed if the US CAPCO classification and marking system is used.

Example of Classification or Marking System: **XYZ Marking System**

4.1.11. Object Country Coding Method

This metadata element identifies the coding method for the Object Country Code (Par. 4.1.12) metadata. The Object Country Coding Method may use FIPS 10-4 two-letter, or four-letter alphabetic country codes or ISO-3166 two-letter, three-letter, or numeric codes for countries, or some other designated coding method. A free text method may also be used. This metadata element is not needed if the default FIPS 10-4 two-letter code is used.

Examples of Country Coding Method: **ISO-3166 Two Letter**
Free Text

4.1.12. Object Country Code

This metadata element contains a value identifying the country that is the object of the essence or metadata to which the Security Metadata Set is linked. Multiple countries may be shown separated by a semi-colon. The default method of coding is the FIPS 10-4 two-letter code.

Example of a Subject Country: AL;HU (Example of default FIPS 10-4 codes)

4.1.13. Comments

This metadata element allows for security related comments and format changes that may be necessary In the future. This field is in addition to those required by CAPCO and is optional.

4.2. Security Metadata Universal Set

The individual metadata elements that comprise information needed to identify the security classification of MPEG-2 streams and other metadata are defined as SMPTE KLV metadata

elements in SMPTE RP210-2000 (Draft submitted). The Security Metadata Universal Set 16-byte Universal Label Key shall be: 06 0E 2B 34 02 01 01 01 02 08 02 00 00 00 00 00[1]. Required security and linking information shall be contained entirely within a Security Metadata Set that conforms to SMPTE 336M KLV encoding rules. The Security Metadata Set shall be a compliant Universal Set as determined by the metadata originator. While it is possible that Security metadata could be expressed as a Global Set, a pack or even as a label, the decision was made to use the Universal Set to reduce ambiguity or chances for misinterpretation.

4.3. Security Metadata Set Application in MPEG-2 Streams

It is imperative that Security Metadata Sets be correctly associated with the information, which they describe by always containing a link to some essence or other metadata. The following metadata elements shall be used to associate Security Metadata Sets with essence (video, audio, data) or other metadata within MPEG-2 TS or PS, which may contain multiple ES material.

4.3.1. Metadata Links within MPEG-2 Streams

Any KLV metadata that conforms to SMPTE 336M (whether individual metadata, sets, or packs) may be linked to MPEG-2 ES within TS or PS using the following unique MPEG-2 stream identifiers:

Unique Material Identifier (UMID)

If used, the 32-byte UMID defined by SMPTE 330M shall be used to identify the essence to which security metadata is linked.

Stream ID — In MPEG-2 Program Streams the 8-bit stream_id specifies the type and number of the Elementary Stream. In MPEG-2 Transport Streams the stream_id may be set by the user to any valid value which correctly describes the Elementary Stream type. (ISO/IEC 13818-1, par 2.4.3.7 and Table 2-18.) The stream_id shall be the Value for the Stream ID metadata element.

Transport Stream ID — When multiple Transport Streams are present in a network environment the 16-bit transport_stream_id uniquely identifies a specific Transport Stream from any other Transport Stream to remove any ambiguity. Its value is defined by the originator. (ISO/IEC 13818-1, par 2.4.4.5.) The transport_stream_id shall be the Value for the Transport Stream ID.

Universal Label Key ID — The 16-byte Universal Label Key for the element, set or pack to which the Security Metadata Set is linked shall be the Value of the Universal Label Key ID.

4.3.2. Linking Security Metadata to MPEG-2 Streams

To indicate the security classification of individual MPEG-2 streams the appropriate link metadata elements shall be contained within a Security Metadata Set as follows:

Elementary Streams– Use of stand-alone ES formats is discouraged for the reasons cited in the MISB RP, *Use of MPEG-2 Systems Streams in Digital Motion Imagery Systems* (DRAFT). However, each Elementary Stream within a Transport Stream or Program Stream shall be associated with a valid Metadata Security Set by containing the one or more UMID or Stream ID

[1] All Set UL Keys (Designators) are tentative and may be changed as the SMPTE Sets Dictionary is developed.

metadata elements for the streams to which they apply. If the same Metadata Security Set applies to multiple Elementary Streams then the Metadata Security Set shall contain each of the UMIDs or Stream IDs separately in the Set.

Transport Streams – Each Transport Stream shall be associated with a valid Metadata Security Set by containing the UMID or Transport Stream ID metadata element for that Transport Stream. The Security Metadata Set for the Transport Stream shall convey all the security information for the highest classification Elementary Stream or metadata contained in the Transport Stream.

Program Streams – The UMID shall be used for directly linking Security metadata to identified Program Streams in their entirety. The Security Metadata Set for the Program Stream shall convey all the security information for the highest classification Transport Stream, Elementary Stream or metadata contained in the Program Stream.

4.3.3. Linking Security Metadata to Other Metadata

When a single metadata element is associated with a Security Metadata Set the Security Metadata Set shall contain Universal Label Key ID whose Value is the 16-byte Universal label Key for the single metadata element.

When some but not all metadata elements within a set or pack must be liked to a Security Metadata Set the Security Metadata Set shall contain each individual Universal Label Key ID for the metadata to which it is linked.

When all metadata in a set or pack is associated with a Security Metadata Set then the set or pack shall contain the Security Metadata Set with a Universal Label Key ID whose value is the Universal Label Key for the set or pack. If all metadata in an Elementary Stream is associated with the same Security Metadata Set then the two shall be associated using the method in 3.3.3 above for Elementary Streams.

4.3.4. Security Metadata Without Links

Security Metadata Sets that do not contain a Stream ID link or a Transport Stream ID link to MPEG-2 streams or a Universal Label Key ID link to other metadata are non-compliant and prohibited. The presence of a stand-alone Security Metadata Set without links is ambiguous and presents a potential security hazard.

4.3.5. Classification of Metadata Security Sets

Every effort shall be made to keep the contents (values) within a Security Metadata Set Unclassified. When one or more elements in a Security Metadata Set must be classified they must be linked to another (or the same) Security Metadata Set by a Universal Label Key ID for the classified element(s).

If an entire Security Metadata Set must be classified it shall be linked to another (or the same) Security Metadata Set by the Universal Label Key ID for itself.

4.3.6. Security Metadata Set Repetition Rate

Security Metadata Sets shall be repeated at regular, short intervals such as every 5, 10, 15, 30, or 60 seconds. The maximum repetition interval shall be 60 seconds. Applications that produce very short motion imagery clips or segments of a few seconds in duration may need to repeat Security Metadata Sets as often as every frame.

4.3.7. Unclassified Essence and Metadata

When essence and/or metadata are unclassified the Security Metadata Set shall consist of the value "UNCLASSIFIED//" for Security Classification. Other entries in the Set that limit or clarify the classification are optional.

4.3.8. Partial Security Metadata Sets

For some classifications (e.g. unclassified, collateral), or other circumstances, not all metadata elements in Par. 4.1 may be required. It is the responsibility of the originator and their cognizant security office to ensure that all appropriate security entries are used.

4.3.9. Absence of Security Metadata Sets in MPEG-2 Streams

The absence of one or more Security Metadata Sets cannot and shall not be construed as rendering an MPEG-2 stream or metadata as Unclassified. The proper insertion of Security Metadata Sets into MPEG-2 streams and the extraction of Security information is the responsibility of system developers. It is the responsibility of bitstream originators and system developers to incorporate continual checks for Security Metadata Sets in their applications.

4.4. Summary of Security Metadata Set Elements

Metadata elements allowed in a Security Metadata Universal Sets are summarized in Table 1.

06 0E 2B 34 01 01 01 03 02 08 02 01 00 00 00 00	Security Classification
06 0E 2B 34 01 01 01 03 07 01 20 01 02 07 00 00	Non-US Classifying Country and Releasing Instructions Country Coding Method
06 0E 2B 34 01 01 01 03 07 01 20 01 02 08 00 00	Non-US Classifying Country
06 0E 2B 34 01 01 01 03 02 08 02 02 00 00 00 00	Caveats
06 0E 2B 34 01 01 01 03 07 01 20 01 02 09 00 00	Release Instructions
06 0E 2B 34 01 01 01 03 02 08 02 03 00 00 00 00	Classified By
06 0E 2B 34 01 01 01 03 02 08 02 04 00 00 00 00	Classification Reason
06 0E 2B 34 01 01 01 03 02 08 02 05 00 00 00 00	Declassification
06 0E 2B 34 01 01 01 03 02 08 02 06 00 00 00 00	Derived From
06 0E 2B 34 01 01 01 03 02 08 02 08 00 00 00 00	Classification or Marking System
06 0E 2B 34 01 01 01 03 07 01 20 01 02 06 00 00	Object Country Coding Method
06 0E 2B 34 01 01 01 03 07 01 20 01 02 01 01 00	Object Country Code
06 0E 2B 34 01 01 01 03 02 08 02 07 00 00 00 00	Classification Comment
06 0E 2B 34 01 01 01 01 01 01 01 XY 00 00 00 00	UMID Video
06 0E 2B 34 01 01 01 01 01 01 02 XY 00 00 00 00	UMID Audio
06 0E 2B 34 01 01 01 01 01 01 03 XY 00 00 00 00	UMID Data
06 0E 2B 34 01 01 01 01 01 01 04 XY 00 00 00 00	UMID System
06 0E 2B 34 01 01 01 03 01 03 04 02 00 00 00 00	Stream ID
06 0E 2B 34 01 01 01 03 01 03 04 03 00 00 00 00	Transport Stream ID
06 0E 2B 34 01 01 01 03 01 03 06 01 00 00 00 00	Item Designator ID (16 byte)

Table 1 - Security Metadata Set Elements

4.5. Security Metadata Set Mapped to NITFS

When a single frame is extracted from an MPEG-2 Video Elementary Stream and is converted into an NITFS image and the associated KLV metadata is used to populate the National Imagery Transmission Format Standard (NITFS) Exploitation Support Data (ESD) the linked Security Metadata Sets shall be compared to determine the highest and/or most restrictive Security Metadata Set and apply that set according to the mapping shown in Table 2.

Metadata Security Set Element	NITFS Field Name(s)	NITF 2.1 Reference
Security Classification	FSCLAS (File Security Classification)	page 58
Non-US Classifying Country and Releasing Instructions Country Code Method	Not applicable	
Non-US Classifying Country	FSCLAS (File Security Classification)	page 58
Caveats	FSCODE (File Codewords) and FSCTLH (File Control and Handling)	page 59
Releasing Instructions	FSREL (File Releasing Instructions)	page 58
Declassification Date	FSDCTP (File Declassification Type) and FSDCDT (File Declassification Date)	page 58
Classified By	FSCATP (File Classification Authority Type) and FSCAUT (File Classification Authority)	page 60
Classification Reason	FSCRSN (File Classification Reason)	page 60
Derived From	FSCATP (File Classification Authority Type) and FSCAUT (File Classification Authority) and FSSRDT (File Security Source Date)	page 60
Classification or Marking System	Not applicable	
Object Country Code Method	Not applicable	
Object Country Code	TBD	
Comments	Not applicable	
UMID (Video Essence)	Not applicable	
UMID (Audio Essence)	Not applicable	
UMID (Data Essence)	Not applicable	
UMID (System)	Not applicable	
Stream ID	Not applicable	
Transport Stream ID	Not applicable	
Universal Label Key ID	Not applicable	

Table 2 - Mapping of Security Metadata Set Elements into NITFS Security Fields

Annex A (Informative) – Security Metadata Set Elements

06	0E	2B	34	01	01	01	03	02	08	02	01	00	00	00	00	Security Classification	Marking of the security level or other description of the classification of information
06	0E	2B	34	01	01	01	03	07	01	20	01	02	07	00	00	Non-US Classifying Country and Releasing Instructions Country Code Method	The coding method used to identify the Non-US classifying country and countries in the releasing instructions
06	0E	2B	34	01	01	01	03	07	01	20	01	02	08	00	00	Non-US Classifying Country	ISO 3166 code of non-US country setting the security classification
06	0E	2B	34	01	01	01	03	02	08	02	02	00	00	00	00	Caveats	Marking of security exceptions or restrictions on the security classification
06	0E	2B	34	01	01	01	03	07	01	20	01	02	09	00	00	Releasing Instructions	ISO 3166 code of countries to which classified information is releasable
06	0E	2B	34	01	01	01	03	02	08	02	03	00	00	00	00	Classified By	Original classification authority name and position or personal identifier; the title of the document or security classification guide used to classify the information
06	0E	2B	34	01	01	01	03	02	08	02	04	00	00	00	00	Classification Reason	Narrative text explaining the reason for assigning the classification
06	0E	2B	34	01	01	01	03	02	08	02	05	00	00	00	00	Declassification	Date for automatic declassification or the code indicating exemption from automatic declassification
06	0E	2B	34	01	01	01	03	02	08	02	06	00	00	00	00	Derived From	Narrative text indicating the source document or authority for derivative declassification
06	0E	2B	34	01	01	01	03	02	08	02	08	00	00	00	00	Classification and Marking System	Classification and marking system used in the Set
06	0E	2B	34	01	01	01	03	07	01	20	01	02	06	00	00	Object Country Code Method	The coding method used to identify the object country code
06	0E	2B	34	01	01	01	03	07	01	20	01	02	01	01	00	Object Country Code	The country code or text that represents the country depicted in the essence.
06	0E	2B	34	01	01	01	03	02	08	02	07	00	00	00	00	Classification Comment	Narrative text further explaining the classification assignment
06	0E	2B	34	01	01	01	01	01	01	01	XY	00	00	00	00	UMID Video	Unique Material Identifier for video essence. Note - the UMID has a 12 byte SMPTE label. XY defines the Material/Instance number creation and/or usage methods.
06	0E	2B	34	01	01	01	01	01	01	02	XY	00	00	00	00	UMID Audio	Unique Material Identifier for audio essence. Note - the UMID has a 12 byte SMPTE label. XY defines the Material/Instance number creation and/or usage methods.
06	0E	2B	34	01	01	01	01	01	01	03	XY	00	00	00	00	UMID Data	Unique Material Identifier for data essence. Note - the UMID has a 12 byte SMPTE label. XY defines the Material/Instance number creation and/or usage methods.
06	0E	2B	34	01	01	01	01	01	01	04	XY	00	00	00	00	UMID System	Unique Material Identifier for other material including grouped picture, audio or data essence. Note - the UMID has a 12 byte SMPTE label. XY defines the Material/Instance number creation and/or usage methods.
06	0E	2B	34	01	01	01	03	01	03	04	02	00	00	00	00	Stream ID	Organizationally given identifier that is the steam_id in ISO/IEC 13818-1 (MPEG-2 Systems)
06	0E	2B	34	01	01	01	03	01	03	04	03	00	00	00	00	Transport Stream ID	Organizationally given identifier that is the transport_stream_id in ISO/IEC 13818-1 (MPEG-2 Systems)
06	0E	2B	34	01	01	01	03	01	03	06	01	00	00	00	00	Item Designator ID (16 byte)	Organizationally given identifier that is the 16-byte Item Designator (SMPTE 336M) for any data or metadata that uses the SMPTE Universal Label